

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

THIS PAGE BLANK (USPTO)

09/926360

JG13 Rec'd PCT/PTO 22 OCT 2001

DOCKET NO.: 214946US2PCT

#4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: PAILLES Jean-Claude et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/FR00/01023

INTERNATIONAL FILING DATE: April 19, 2000

FOR: PAYMENT SYSTEM FOR SOFTWARE PROGRAM USE

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119
AND THE INTERNATIONAL CONVENTION**Assistant Commissioner for Patents
Washington, D.C. 20231

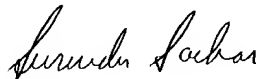
Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

COUNTRY
France**APPLICATION NO**
99 04963**DAY/MONTH/YEAR**
20 April 1999

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/FR00/01023. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,
OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak
Attorney of Record
Registration No. 24,913
Surinder Sachar
Registration No. 34,423



22850

(703) 413-3000
Fax No. (703) 413-2220
(OSMMN 1/97)

THIS PAGE BLANK (USPTO)

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

T/FR 00 / 0 1 0 2 3

26 AVR. 2000

REC'D 15 MAY 2000

WIPO PCT

FR 00/1023

EJU

B R E V E T D ' I N V E N T I O N**CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION****09/926360****COPIE OFFICIELLE**

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 18 AVR. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

A handwritten signature in black ink, appearing to read 'M. Planche', enclosed within a large, loopy oval stroke.

Martine PLANCHE

**INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE**

SIEGE

26 bis, rue de Saint Petersburg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

THIS PAGE BLANK (USPTO)

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES

20 AVR 1999

N° D'ENREGISTREMENT NATIONAL

99 04963

DÉPARTEMENT DE DÉPÔT

DATE DE DÉPÔT

20 AVR. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

**SOCIÉTÉ DE PROTECTION
DES INVENTIONS
03, rue du Docteur Lancereaux
75008 PARIS**

n° du pouvoir permanent SP 16448.C/RS 01 53 83 94 00
c/03100

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention

☐ demande divisionnaire

☐ demande initiale

☐ certificat d'utilité

☐ transformation d'une demande
de brevet européen

☐ brevet d'invention

☐ certificat d'utilité n°

date

Établissement du rapport de recherche

☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance

☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

SYSTEME DE PAIEMENT POUR L'UTILISATION DE LOGICIELS.

3 DEMANDEUR (S) n° SIREN

code APE-NAF

Norm et prénoms (souligner le nom patronymique) ou dénomination

FRANCE TELECOM

Forme juridique

Société Anonyme

Nationalité (s) Française

Adresse (s) complète (s)

6 Place d'Alleray 75015 PARIS

Pays

France

En cas d'insuffisance de place, poursuivre sur papier libre

4 INVENTEUR (S) Les inventeurs sont les demandeurs

☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES

☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine

numéro

date de dépôt

nature de la demande

7 DIVISIONS

antérieures à la présente demande n°

date

n°

date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE

(nom et qualité du signataire)

**D. PUJOLISBAUDRY
CPI 950 304**

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Petersbourg SP 16448.C/RS
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

9904963

TITRE DE L'INVENTION :

SYSTEME DE PAIEMENT POUR L'UTILISATION DE LOGICIELS.

LE(S) SOUSSIGNÉ(S)

D. DU BOISBAUDRY
c/o SOCIÉTÉ DE PROTECTION
DES INVENTIONS
25 rue de Ponthieu
75008 PARIS

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

PAILLES Jean-Claude

4, rue des Loisirs
14610 EPRON

MICHON Philippe

96 avenue H. Cheron
14000 CAEN

PETIT Stéphane

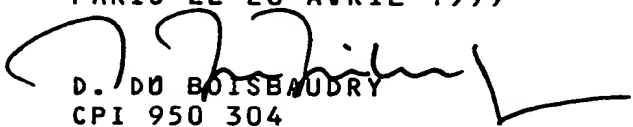
App.146, Bât Les Iris
Rés. du Nouveau Bassin
32 rue de Ver
14470 COURSEULES/MER

FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

PARIS LE 20 AVRIL 1999


D. DU BOISBAUDRY
CPI 950 304

SYSTEME DE PAIEMENT POUR L'UTILISATION DE LOGICIELS
DESCRIPTION

Domaine technique

5 La présente invention a pour objet un système de paiement pour l'utilisation de logiciels. Ces logiciels peuvent être de nature quelconque et par exemple être des logiciels enregistrés sur un support comme les CD-ROM (Compact Disc-Read Only Memory) ou les
10 DVD-ROM (Digital Versatile Disc-Read Only Memory) ou les logiciels téléchargés.

 Ils peuvent concerner aussi bien des calculs scientifiques que des jeux, des techniques assistées par ordinateur, du traitement de texte, etc..

15

Etat de la technique antérieure

 Le mode actuel de diffusion des logiciels est principalement le CD-ROM, et sera très bientôt le DVD-ROM. Pour les éditeurs de logiciel se pose de façon
20 de plus en plus aiguë le problème de la copie frauduleuse de ces logiciels. Si, pendant un temps, le format du CD-ROM a empêché la recopie sur un support vierge, actuellement, les disques inscriptibles et les graveurs de CD sont devenus accessibles au niveau du
25 grand public. Le même phénomène ne tardera sans doute pas à advenir dans le cas de la technologie DVD.

 Un autre mode possible de diffusion des logiciels, quoique moins usité pour des raisons de performances, est le téléchargement. Il n'est pas
30 approprié aux jeux ayant besoin de très nombreuses images, ou scènes en trois dimensions. En revanche, il peut se justifier dans d'autres cas. De nombreux

logiciels (compilateurs, éditeurs...) entrent dans cette catégorie. Ces logiciels sont en général gratuits, car, du fait de leur volume faible qui les rend téléchargeables, ils seraient très faciles à copier d'un ordinateur à un autre.

Par ailleurs, il est clair que le prix d'achat élevé d'un logiciel est souvent dissuasif pour les utilisateurs. Le coût du support CD-ROM et de sa gravure intervient pour très peu dans ce prix. Le prix d'achat élevé des CD/DVD-ROM actuels correspond avant tout à la rémunération de l'éditeur et des distributeurs des jeux.

Ces observations donnent à penser qu'il existe un besoin pour le paiement à l'acte, ou à la durée ou à la séance de logiciels sur support CD/DVD-ROM, ou des logiciels téléchargés. Ainsi, les éditeurs se rémunéreront sur une base de clients beaucoup plus importante, en fonction de l'utilisation que le client fait de ce logiciel. Globalement, un tel procédé devrait plutôt développer le chiffre d'affaires de la profession. De plus, la copie de support ne présentera plus d'intérêt, puisque de toute façon, il sera nécessaire de payer pour l'utilisation de ce logiciel.

Or, il n'y a pas, à l'heure actuelle de moyens fiables et sûrs pour assurer un paiement pour l'utilisation de logiciels. La présente invention a justement pour but de remédier à cette carence.

Exposé de l'invention

Un système de paiement pour l'utilisation de logiciel doit pouvoir remplir au moins trois fonctions :

- 5 ° contrôler l'utilisation du logiciel, chaque fois que le logiciel est lancé, ou bien périodiquement, ou bien lorsqu'un événement particulier se produit dans le logiciel (par exemple un changement de "monde" dans un jeu, un passage au deuxième acte d'une pièce de théâtre ou de film...) ; alors, le logiciel doit demander qu'un paiement soit effectué ;
- 10 ° enregistrer les utilisations, pour faire payer l'utilisateur : si l'utilisateur accepte la demande de paiement, il faut enregistrer cette demande d'une façon sécurisée, pour pouvoir le faire payer ultérieurement ; la sécurisation doit interdire à l'utilisateur d'effacer ses dettes, et le paiement différé doit permettre d'agréger des petits montants,

15 pour pouvoir présenter à l'utilisateur une note globale, périodiquement (une fois par mois, par exemple), pour des raisons pratiques mais aussi du fait des coûts de recouvrement de ces petits montants ;
- 20 ° reverser périodiquement à l'éditeur du logiciel le montant dû.

Ces fonctions doivent être remplies compte tenu de certaines contraintes :

- 25 ° les CD-ROM peuvent être étrangers : un système de paiement de logiciel doit donc comporter une dimension trans-frontière, donc des mécanismes susceptibles d'être déployés internationalement, et une reconnaissance internationale dans des comités de standardisation ;
- 30 ° l'interface entre logiciel et les moyens de paiement doit être standardisée de façon à ce qu'un

développeur de logiciel n'ait pas à programmer lui-même la logique de paiement correspondant à l'emploi de ce logiciel ;

- 5 • le système qui enregistre les utilisations doit être capable de déclencher des paiements internationaux pour rémunérer les éditeurs de logiciels dans n'importe quel pays du monde ;
- 10 • l'agrégation pour les paiements des utilisateurs et les reversements aux éditeurs de logiciels doit être possible : comme indiqué plus haut, ceci correspond à un objectif de simplicité, mais aussi à un souci de réduction des coûts bancaires ; notamment, dans le cas de transactions vers l'étranger, il serait inefficace (voire néfaste), sur le plan des coûts, de
15 faire trop d'opérations de virements de petits montants.

La présente invention répond à toutes ces exigences en tenant compte de toutes ces contraintes. A
20 cette fin, le système de l'invention comprend un module de paiement et des moyens de traitement de messages et de paiement. Par ailleurs, le logiciel dont on veut contrôler l'utilisation comprend une interface logicielle. Les fonctions de ces moyens sont les
25 suivantes :

- l'interface logicielle est apte à constituer un premier message qui est un message d'offre d'utilisation du logiciel, ce premier message contenant, notamment, l'identité de l'éditeur du
30 logiciel, les paramètres de l'offre, la signature numérique par l'éditeur d'au moins une partie de

l'offre, ce premier message étant adressé au module de paiement ;

- 5 ° le module de paiement est apte à recevoir ce premier message, à l'afficher, à recevoir en retour l'acceptation éventuelle de l'utilisateur du logiciel, et, en cas d'acceptation, à constituer un deuxième message de demande de paiement contenant notamment l'identité de l'utilisateur et celle de l'éditeur, ainsi qu'une preuve que l'utilisateur
10 accepte l'offre, ce module étant apte à adresser ce deuxième message aux moyens de traitement ;
- 15 ° les moyens de traitement de messages et de paiement sont aptes à recevoir le deuxième message, à contrôler la preuve qu'il contient, à enregistrer la demande de paiement avec au moins l'identité de l'utilisateur et l'identité de l'éditeur du logiciel, le montant à payer, et à créditer l'éditeur dudit
20 montant, ces moyens étant aptes en outre à constituer un troisième message, qui est un message d'acquiescement, ce troisième message comprenant, notamment, l'identité des moyens de traitement et une signature numérique de l'offre, ce troisième message étant adressé au module de paiement ;
- 25 ° le module de paiement est en outre apte à retransmettre ce troisième message à l'interface logicielle ;
- 30 ° l'interface logicielle est en outre apte à vérifier la signature des moyens de traitement par rapport aux paramètres de l'offre contenue dans le premier message et, en cas de concordance, à autoriser l'utilisation du logiciel.

Dans une première variante, les moyens de traitement de messages et de paiement sont constitués par un serveur de paiement distant relié au module de paiement par un réseau de télécommunications, ce
5 serveur recevant et traitant le deuxième message, constituant et émettant le troisième message. Ce serveur de paiement agrège les crédits élémentaires pour, périodiquement, reverser aux éditeurs le montant qui leur est dû.

10 Dans une seconde variante les moyens de traitement de messages et de paiement comprennent des moyens sécurisés contenant au moins l'identité de l'utilisateur, ces moyens étant de plus aptes à recevoir le deuxième message, à contrôler la preuve
15 qu'il contient, à enregistrer la demande de paiement et à constituer le troisième message d'acquiescement, et comprennent en outre un serveur de paiement distant apte à créditer l'éditeur.

Dans cette variante, les moyens sécurisés
20 peuvent comprendre un lecteur de carte à puce avec une carte à puce contenant l'identité de l'utilisateur, la carte étant apte à recevoir le deuxième message, à contrôler la preuve qu'il contient, à enregistrer la demande de paiement et à constituer le troisième
25 message d'acquiescement.

Régulièrement, l'ensemble des demandes enregistrées dans la carte, qui correspondent à des usages de logiciels, sont rapatriées dans le serveur grâce à un réseau de télécommunications.

30 La carte peut être du type prépayée (sous forme par exemple de porte monnaie électronique) ou postpayée.

Brève description des figures

- la figure 1 illustre un système conforme à l'invention dans sa première variante ;

5 - la figure 2 illustre un arbre de certification avec une chaîne de certificats ;

- la figure 3 illustre un système conforme à l'invention dans sa seconde variante.

10 Description détaillée de modes particuliers de réalisation

On voit, sur la figure 1, un ordinateur personnel PC supposé contenir un logiciel L, dont on veut contrôler l'utilisation. Ce logiciel est associé à
15 une interface logicielle IL, appelée par la suite "MARCHAND", qui communique avec le système de paiement proprement dit. On trouve également un module de paiement W, appelé par la suite "WALLET". A distance se trouve un serveur de paiement SP, relié au module
20 WALLET par une ligne de transmission (non représentée). L'éditeur du logiciel est référencé E.

Dans la variante illustrée sur la figure 1, lorsque le logiciel L a décidé de demander un nouveau paiement, un message d'offre référencé 1 est émis par
25 l'interface MARCHAND à destination du module WALLET. Ce message d'offre peut contenir :

- l'identité de l'éditeur ;
- la description de l'offre, texte compréhensible par l'utilisateur explicitant ce qu'il va obtenir
30 moyennant paiement (par exemple : "30 minutes

supplémentaires d'utilisation" ou bien "scène 3 : durée 25 minutes") ;

- le prix (montant, unité monétaire, etc.)
- l'heure et la date interne du PC ;
- 5 • un aléa interne ;
- une signature par l'éditeur du logiciel de cette offre, sous la forme $S_E(\text{offre}_h, \text{prix})$ où offre signifie "condensé des données de l'offre".

Le module WALLET recevant ce message va
 10 demander à l'utilisateur U s'il est d'accord pour accepter cette offre. Par exemple, une fenêtre est affichée à l'écran, visualisant la description de l'offre, l'heure et la date, le montant et l'unité monétaire à payer, et ce même prix converti en Francs
 15 français. Cet affichage est symbolisé par la flèche la sur la figure 1.

Si l'utilisateur U est d'accord, il clique par exemple sur une case " accord " (réponse symbolisée par la flèche 1b sur la figure 1). Le module WALLET émet
 20 alors le message 2 "demande de paiement" à destination du serveur SP. Ce message peut contenir :

- un condensé de l'offre_h , le prix, la date et l'heure, l'aléa, la signature $S_E(\text{offre}_h, \text{prix})$;
- l'identité de l'utilisateur U, et celle de l'éditeur
 25 E ;
- une preuve que le client est d'accord pour acheter cette offre. La nature de la preuve peut dépendre du mode de réalisation : ce peut être un mot de passe envoyé au serveur de paiement SP, ou un code
 30 confidentiel donné à une carte à puce, qui elle-même

fournit au serveur SP une preuve cryptographique : signature, etc..

Le fait de transmettre un condensé de l'offre ("offre_h") et non l'offre complète permet au client de
 5 ne pas révéler au serveur SP ce qu'il sélectionne, sans empêcher les contrôles par le serveur SP.

Le serveur de paiement SP recevant cette demande de paiement 2 effectue alors les opérations suivantes :

- 10 ◦ contrôle de la preuve donnée par le client,
- conversion en Francs français, si nécessaire,
- contrôle de la consommation de l'utilisateur ; à titre d'exemple, le serveur SP vérifie que le cumul de ce qui a été consommé depuis le début de la
 15 période est inférieur au montant d'autorisation attribué à cet utilisateur (cas du post-paiement), ou bien que ce cumul est inférieur à la provision constituée par l'utilisateur à cet usage (cas du pré-paiement),
- 20 ◦ enregistrement de la demande de paiement, pour pouvoir réaliser ultérieurement les opérations de paiement ; cet enregistrement comporte au moins :
 - l'identification de l'utilisateur,
 - l'identification de l'éditeur du logiciel,
 - 25 -le prix,
 - l'heure et date, le condensé offre_h,
- constitution du message 3 d'acquiescement, qui va prouver au logiciel et à son interface "MARCHAND" que le paiement a bien été réalisé ; ce message
 30 d'acquiescement, pour établir une preuve vérifiable, contiendra :

-l'identité du serveur SP,
-la signature S_{SP} ($offre_h$, prix, aléa, date-
heure) par le serveur de paiement,

Le module WALLET transmet simplement le
5 message reçu à l'interface MARCHAND.

L'interface MARCHAND vérifie la signature
 $S_{SP}(offre_h, \text{prix}, \text{aléa}, \text{date-heure})$ du message
d'acquiescement, par rapport aux paramètres de l'offre
précédemment envoyée. S'il y a concordance, alors
10 l'exécution du logiciel L peut continuer.

Périodiquement, tous les mois par exemple, le
serveur SP calcule le cumul des dépenses engagées par
chaque utilisateur, et il provoque, dans le cas d'un
post-paiement, le paiement effectif des sommes dues au
15 moyen d'une carte pour lequel la connaissance préalable
du numéro de carte du client est nécessaire, ou par
prélèvement automatique sur le compte du client.

Pour le pré-paiement, ceci se fait par le
rechargement volontaire par l'utilisateur de sa
20 provision chez un intermédiaire.

De même, le cumul par l'éditeur permet de
calculer le montant dû à chaque éditeur.

Les traits pointillés du dessin de la figure 1
correspondent à ce flux financier du serveur SP vers
25 l'éditeur.

Pour l'établissement des différentes
signatures mentionnées ci-dessus, on peut utiliser un
système à clé publique avec arbre de certification.
30 Cette solution est en effet l'une des rares qui

permettent de concevoir des systèmes simples, sûrs, ouverts et internationalement reconnus.

Les principes de cette technique sont bien connus. La mise en œuvre est schématisée sur la figure 2. Une autorité A définit la "racine" de l'arbre de certification, dans lequel se trouvent les différents acteurs du système :

- les éditeurs de logiciels utilisant ce moyen de paiement,
- 10 - les serveurs SP,
- les entités intermédiaires ; dans l'exemple de la figure 2, il pourrait s'agir d'un syndicat d'éditeurs de logiciels d'un pays (SYND), et d'une autorité nationale de
- 15 régulation des serveurs INTERNET (SINT).

Ainsi, lorsqu'un logiciel de tel éditeur de logiciel est utilisé par un utilisateur correspondant à tel serveur SP, des certificats joints aux messages 2 et 3 permettent de vérifier les signatures.

20 Pour le message d'offre (message 2) l'éditeur E peut adresser au serveur SP un message contenant le condensé offre_h , le prix, la date et l'heure, l'aléa, la signature $S_E(\text{offre}_h, \text{prix})$, le certificat de E par SYND, le certificat de SYND par A.

25 Le serveur SP, qui connaît la clé publique de A, vérifie le certificat de SYND par A, avec la clé publique de A. Il obtient donc la clé publique de SYND, de façon sûre et vérifie le certificat de E par SYND avec la clé publique de SYND. Il obtient alors la clé

30 publique de E, de façon sûre, et peut finalement contrôler la signature S_E .

La variante qui vient d'être décrite peut être qualifiée de "en ligne" ("on line") car l'utilisateur doit se connecter, par exemple par le réseau INTERNET, au serveur SP à chaque demande de paiement. Cette version n'est acceptable que pour des paiements peu fréquents (par exemple pour pouvoir recevoir un film sur DVD-ROM qui dure 2 heures).

L'invention prévoit une autre variante, qui est mieux appropriée aux paiements répétés. Cette variante est décrite sur la figure 3. Elle suppose l'existence d'un lecteur de carte LC et d'une carte C. Comme la carte constitue un support sûr, elle remplace le serveur SP en ce qui concerne les messages 2 et 3, lesquels circulent alors entre le module W et le lecteur de carte LC. Cette variante peut être qualifiée de "off line" (hors connexion) par opposition à la première. Le paiement de l'éditeur E s'effectue toujours par le serveur de paiement SP, lequel reçoit périodiquement les informations mémorisées dans la carte (ligne PP).

S'agissant de la carte C, on peut distinguer deux cas :

- la carte est une carte pré-payée (du type carte porte-monnaie électronique, par exemple) ; la provision financière diminue à chaque fois qu'un message de demande de paiement est traité ; alors, il n'y a pas de risque d'impayés, car la carte avant de se vider, a du être chargée ; il faut cependant relever les utilisations qui ont été faites, pour pouvoir payer les éditeurs, selon l'utilisation de

leurs jeux ; ceci peut par exemple être fait au moment du rechargement de la carte ;

- la carte est une carte post-payée : le risque existe que les utilisations enregistrées dans la carte ne reviennent jamais à l'intermédiaire, donc que le client ne soit jamais débité, et par voie de conséquence que les éditeurs des logiciels utilisés ne soient pas crédités. La parade à ce problème consiste à limiter les paiements à un certain plafond et/ou à faire payer une caution supérieure à ce plafond, qui dissuade l'utilisateur de faire disparaître sa carte.

Du point de vue des mécanismes précis, cette seconde variante reste très proche de la première, si ce n'est le remplacement du serveur SP par la carte C. Cette carte devra donc contenir un fichier des utilisations qui, comme dans le cas du serveur SP, contiendra les enregistrements des transactions, eux mêmes contenant au minimum les informations suivantes :

- l'identification de l'utilisateur,
- l'identification de l'éditeur du logiciel,
- le prix.

Si l'on accepte de sacrifier un peu de sécurité pour ne pas avoir le surcoût du lecteur de carte, la carte pourra être remplacée par un moyen de mémorisation intégré au PC.

Pour que le fichier des demandes de paiement ne soit pas trop facilement altérable ou effaçable, il faut utiliser des techniques de fragmentation/dissémination sur la totalité du disque, dont la

complexité constituera une barrière, certes moins forte que la sécurité physique des cartes à puce, mais suffisante dans bien des cas.

REVENDICATIONS

1. Système de paiement pour l'utilisation d'un logiciel (L) contenu sur un support, ce logiciel
5 contenant une interface (IL), le système comprenant un module de paiement (W) et des moyens de traitement de messages et de paiement (SP), les fonctions de ces moyens étant les suivantes :
- 10 ◦ l'interface logicielle (IL) est apte à constituer un premier message (1) qui est un message d'offre d'utilisation du logiciel, ce premier message (1) contenant, notamment, l'identité de l'éditeur du logiciel (E), des paramètres de l'offre, la signature numérique par l'éditeur d'au moins une partie de
15 l'offre, ce premier message étant adressé au module de paiement ;
 - 20 ◦ le module de paiement (W) est apte à recevoir ce premier message (1), à l'afficher (1a), à recevoir en retour l'acceptation éventuelle de l'utilisateur (U) du logiciel (1b), et en cas d'acceptation, à constituer un deuxième message (2) de demande de paiement contenant notamment l'identité de l'utilisateur (U) et celle de l'éditeur (E) ainsi qu'une preuve que l'utilisateur (U) accepte l'offre,
25 ce module (W) étant apte à adresser ce deuxième message (2) aux moyens de traitement (SP) ;
 - 30 ◦ les moyens de traitement de messages et de paiement (SP) sont aptes à recevoir le deuxième message (2), à contrôler la preuve qu'il contient, à enregistrer la demande de paiement avec au moins l'identité de l'utilisateur (U) et l'identité de l'éditeur du

- logiciel (E), le montant à payer et à créditer l'éditeur (E) dudit montant, ces moyens étant aptes en outre à constituer un troisième message (3), qui est un message d'acquiescement, ce troisième message
- 5 (3) comprenant, notamment, l'identité des moyens de traitement et une signature numérique qui constitue la preuve du paiement, ce troisième message étant adressé au module de paiement W ;
- le module de paiement (W) est en outre apte à
- 10 retransmettre ce troisième message (3) à l'interface logicielle (IL) ;
- l'interface logicielle (IL) est en outre apte à vérifier la signature des moyens de traitement par rapport aux paramètres de l'offre contenue dans le
- 15 premier message et, en cas de concordance, à autoriser l'utilisation du logiciel (L).

2. Système selon la revendication 1, dans lequel les moyens de traitement de messages et de

20 paiement sont constitués par un serveur de paiement distant (SP) relié au module de paiement (W) par un réseau de télécommunications, ce serveur (SP) recevant et traitant le deuxième message (2) et constituant et émettant le troisième message (3).

25

3. Système selon la revendication 1, dans lequel les moyens de traitement de messages et de paiement comprennent des moyens sécurisés (LC,C) contenant au moins l'identité de l'utilisateur (U), ces

30 moyens étant aptes à recevoir le deuxième message (2), à contrôler la preuve qu'il contient, à enregistrer la

demande de paiement et à constituer le troisième message d'acquiescement (3) avec la preuve de paiement, et comprennent en outre un serveur de paiement distant (SP) apte à créditer l'éditeur (E).

5

4. Système selon la revendication 3, dans lequel les moyens sécurisés comprennent un lecteur de carte (LC) avec une carte (C) contenant l'identité de l'utilisateur, le lecteur de carte et la carte étant aptes à recevoir le deuxième message (2), à contrôler la preuve qu'il contient, à enregistrer la demande de paiement et à constituer le troisième message d'acquiescement (3) avec la preuve de paiement.

15

5. Système selon la revendication 4, dans lequel la carte (C) est du type prépayée et contient une provision, la carte étant apte à débiter cette provision à chaque demande de paiement du montant de la demande.

20

6. Système selon la revendication 5, dans lequel la carte prépayée (C) formant le message d'acquiescement contient une preuve que le montant de la demande dû a été débité dans la carte.

25

7. Système selon la revendication 5, dans lequel la carte prépayée (C) est apte à constituer un fichier des demandes acquiescées et des montants correspondants, le message d'acquiescement n'étant émis avec sa signature qu'une fois la mise à jour de ce fichier effectuée.

30

8. Système selon la revendication 7, dans lequel la carte prépayée (C) peut être rechargée, le fichier qu'elle contient étant transféré préalablement au serveur de paiement (SP) lors du rechargement.

5

9. Système selon la revendication 5, dans lequel la carte prépayée (C) est du type porte-monnaie électronique.

10

10. Système selon la revendication 4, dans lequel la carte (C) est du type post-payée.

FIG. 1

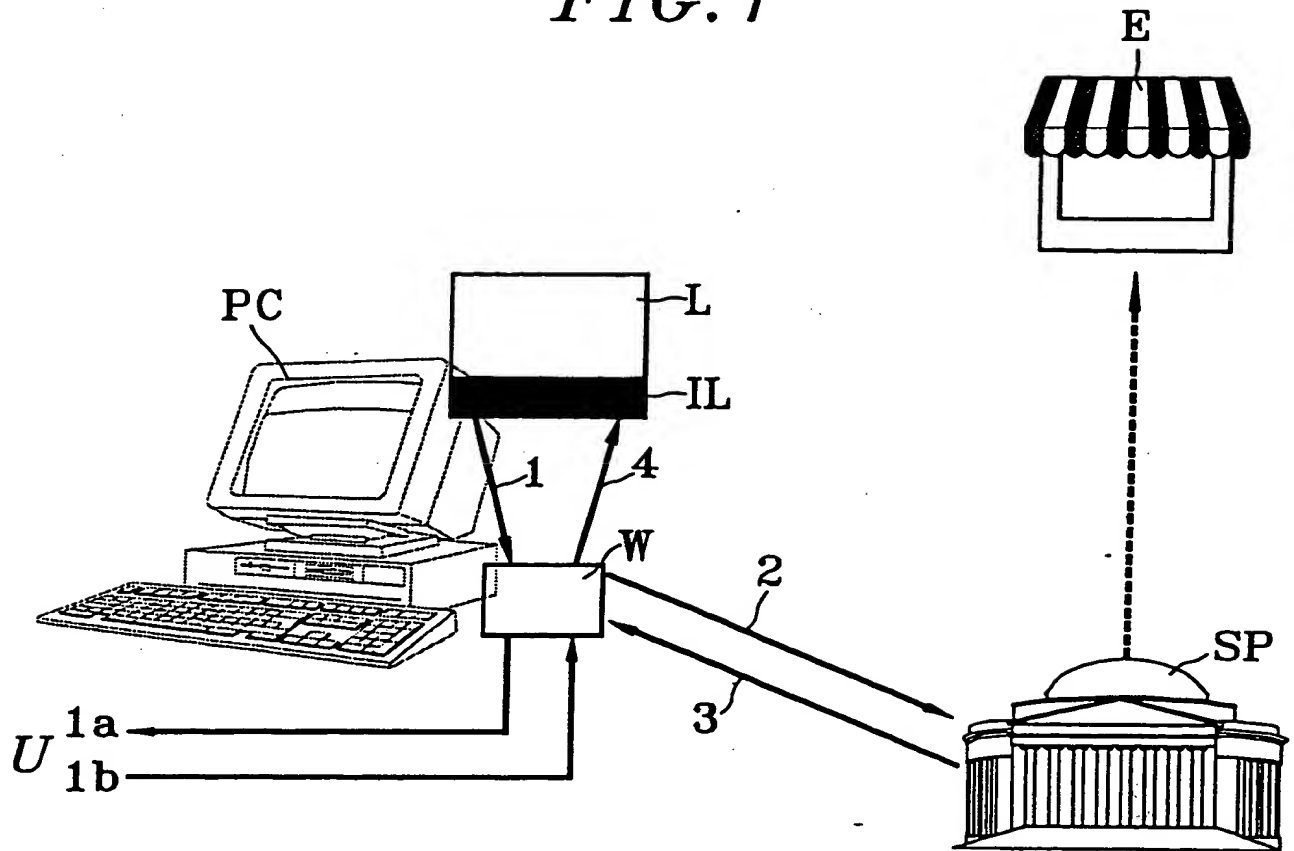


FIG. 2

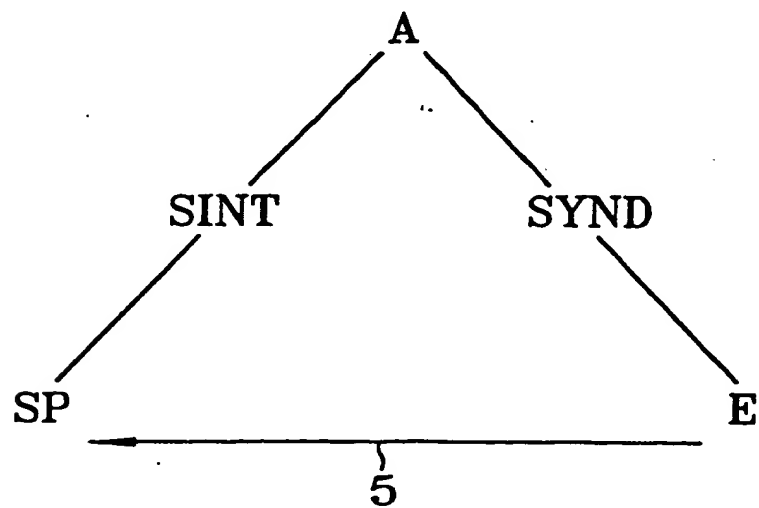


FIG. 3

